

WHAT IS CLAIMED IS:

- 1 1. A peer-to-peer method for performing and managing backups
2 in a network of nodes which form a cooperative collection of machines having
3 excess storage capacity, the method comprising:
4 (a) determining a plurality of peer nodes from the network of
5 nodes for a first node of the network based on an amount of stored data common to
6 both the first node and each of the plurality of peer nodes; and
7 (b) storing a backup copy of data unique to the first node on each
8 of the plurality of peer nodes so that each of the plurality of peer nodes stores a
9 substantially complete backup of the first node.
- 1 2. The method as claimed in claim 1, further comprising
2 repeating steps (a) and (b) for each of the other nodes of the network so that a
3 plurality of substantially complete backups are stored on a plurality of peer nodes
4 for each of the nodes of the network.
- 1 3. The method as claimed in claim 1, wherein the step of
2 determining is also based on network distance that each of the plurality of peer
3 nodes is from the first node.
- 1 4. The method as claimed in claim 1, wherein at least one of the
2 plurality of peer nodes is the local peer node to reduce network load and improve
3 restore performance.
- 1 5. The method as claimed in claim 1, wherein at least one of the
2 plurality of peer nodes is a remote peer node to provide geographic diversity.
- 1 6. The method as claimed in claim 1, wherein data is stored in
2 the first and peer nodes as chunks of data.
- 1 7. The method as claimed in claim 1, further comprising
2 monitoring the plurality of peer nodes to determine if a peer node is no longer

3 capable of providing a backup to the first node and repeating steps (a) and (b) to
4 determine a replacement peer node from the network of nodes and to store a backup
5 copy of data unique to the first node on the replacement peer node.

1 8. The method as claimed in claim 7, wherein the step of
2 monitoring is performed statistically.

1 9. The method as claimed in claim 1, further comprising
2 preventing a forged request to drop a backup copy from one of the peer nodes.

1 10. The method as claimed in claim 6, wherein the data is stored
2 in the peer nodes as encrypted chunks.

1 11. The method as claimed in claim 10, wherein the data is
2 encrypted by a key derived from the data stored in the peer nodes.

1 12. The method as claimed in claim 11, wherein the key is
2 encrypted.

1 13. The method as claimed in claim 12, wherein the key is
2 encrypted by a key-encrypting key stored with the data.

1 14. The method as claimed in claim 2, wherein data is stored in
2 the peer nodes as chunks of encrypted data and wherein each of the encrypted
3 chunks includes data which represents a set of nodes having an interest in the
4 encrypted chunk.

1 15. The method as claimed in claim 1, further comprising
2 determining when the first node is decommissioned and reclaiming storage space on
3 the peer nodes associated with the decommissioned node.

1 16. The method as claimed in claim 1, further comprising
2 determining whether a node of the network claiming to be a peer node is a peer
3 node.

1 17. A peer-to-peer system for performing and managing backups
2 in a network of nodes which form a cooperative collection of machines having
3 excess storage capacity, the system comprising:

4 means for determining a plurality of peer nodes from the network of
5 nodes for a first node of the network based on an amount of stored data common to
6 both the first node and each of the plurality of peer nodes; and

7 means for storing a backup copy of data unique to the first node on
8 each of the plurality of peer nodes so that each of the plurality of peer nodes stores
9 a substantially complete backup of the first node.

1 18. The system as claimed in claim 17, wherein the means for
2 determining determines a plurality of peer nodes from the network for each of the
3 nodes of the network and wherein the means for storing stores a backup copy of data
4 unique to each of the nodes of the network on each of its plurality of peer nodes so
5 that a plurality of substantially complete backups are stored on a plurality of peer
6 nodes for each of the nodes of the network.

1 19. The system as claimed in claim 17, wherein the means for
2 determining determines the plurality of peer nodes based on network distance that
3 each of the plurality of peer nodes is from the first node.

1 20. The system as claimed in claim 17, wherein at least one of the
2 plurality of peer nodes is the local peer node to reduce network load and improve
3 restore performance.

1 21. The system as claimed in claim 17, wherein at least one of the
2 plurality of peer nodes is a remote peer node to provide geographic diversity.

1 22. The system as claimed in claim 17, wherein data is stored in
2 the first and peer nodes as chunks of data.

1 23. The method as claimed in claim 17, further comprising means
2 for monitoring the plurality of peer nodes to determine if a peer node is no longer
3 capable of providing a backup to the first node, wherein the means for determining
4 determines a replacement peer node from the network of nodes and wherein the
5 means for storing stores a backup copy of data unique to the first node on the
6 replacement peer node.

1 24. The system as claimed in claim 23, wherein the means for
2 monitoring monitors the plurality of peer nodes statistically.

1 25. The system as claimed in claim 17, further comprising means
2 for preventing a forged request to drop a backup copy from one of the peer nodes.

1 26. The system as claimed in claim 22, wherein the data is stored
2 in the peer nodes as encrypted chunks.

1 27. The system as claimed in claim 26, wherein the data is
2 encrypted by a key derived from the data stored in the peer nodes.

1 28. The system as claimed in claim 27, wherein the key is
2 encrypted.

1 29. The system as claimed in claim 28, wherein the key is
2 encrypted by a key-encrypting key stored with the data.

1 30. The system as claimed in claim 18, wherein data is stored in
2 the peer nodes as chunks of encrypted data and wherein each of the encrypted
3 chunks includes data which represents a set of nodes having an interest in the
4 encrypted chunk.

1 31. The system as claimed in claim 17, further comprising means
2 for determining when the first node is decommissioned and means for reclaiming
3 storage space on the peer nodes associated with the decommissioned node.

1 32. The system as claimed in claim 17, further comprising means
2 for determining whether a node of the network claiming to be a peer node is a peer
3 node.